



Internal Audit Report

**MIHS Claims System
July 2003**



Audit Team Members

Sandy Chockey, Audit Manager

KPMG LLP

Protiviti, Inc.



Maricopa County

Internal Audit Department

301 West Jefferson St
Suite 1090
Phx, AZ 85003-2143
Phone: 602-506-1585
Fax: 602-506-8957
www.maricopa.gov

July 24, 2003

Fulton Brock, Chairman, Board of Supervisors
Don Stapley, Supervisor, District II
Andrew Kunasek, Supervisor, District III
Max W. Wilson, Supervisor, District IV
Mary Rose Wilcox, Supervisor, District V

We have completed our FY 2002-03 review of the Maricopa Integrated Health System (MIHS) Claims System. The audit was performed in accordance with the annual audit plan that was approved by the Board of Supervisors.

The highlights of this report include the following:

- Access security controls need to be improved to protect sensitive information
- Controls over program changes and segregation of duties should be improved
- The most current software updates have not been installed to the claims system

Attached are the report summary, detailed findings, recommendations, and MIHS management's response. We have reviewed this information with MIHS management and appreciate the excellent cooperation provided by their staff. If you have questions, or wish to discuss items presented in this report, please contact Sandy Chockey at 506-1006.

Sincerely,

A handwritten signature in cursive script that reads "Ross L. Tate".

Ross L. Tate
County Auditor

(Blank Page)

Table of Contents

Executive Summary	1
Introduction	2
Department Accomplishments	4
Detailed Information	5
Department Response	12

Executive Summary

Claims System Security (Page 5)

The current claims system lacks effective security controls over user access, system settings, and password parameters. Weak controls over these areas could result in improper disclosure of information. MIHS should strengthen system security controls.

Program Change Controls (Page 7)

The current claims system lacks effective controls over changes to programs. The absence of change and approval documentation, and effective segregation of duties, increases the risk that a program could cause system failure, malfunction, or inaccurate data. MIHS should improve change control procedures.

System Software (Page 8)

The most current software updates have not been installed for the claims system. In addition, software maintenance procedures are not performed on a regular basis. These weaknesses could result in undetected errors or a disruption of business services. MIHS should strengthen controls over system software maintenance activities.

Regulatory Compliance (Page 10)

New healthcare regulations require increased security controls over systems that contain patient information. Some required controls have not yet been implemented. Incomplete security controls increase the risk that MIHS will not be able to meet regulatory requirements. MIHS should identify the additional work to be done and schedule it for completion prior to statutory deadlines.

System Recovery (Page 11)

System recovery procedures have not been documented and included in the Systems Recovery Procedures or Disaster Recovery Plan. In the event of a disruption of service, MIHS may not be able to recover the system and application in an efficient and timely manner. MIHS should include detailed restoration instructions for the operating system and the claims application in the System Recovery Procedures and the Disaster Recovery Plan.

Introduction

Background

The MC400 system (new claims system) is a suite of healthcare software modules developed by OAO Healthcare Solutions, Inc. (OAOHS). The most significant modules include Member Services, Provider Services, Benefits Management, Finance, Prior Authorization, Case Management, and Medical Management. These modules are integrated using a common database and processing framework. The system is processed on the IBM AS/400 computing architecture.

Maricopa Integrated Health Systems (MIHS) began a project to implement the new claims system in January 2001 to replace multiple legacy applications processing both internally and at an outside Application Service Provider (ASP). A primary driver for the project was to comply with the Health Insurance Portability and Accountability Act (HIPAA), which could not be achieved with the legacy systems. The original project budget was slightly over \$7 million, and was scheduled to “go live” in March 2002. A cross-functional project team was formed from functional and technical areas, as well as from the vendor.

MIHS contracted with OAOHS to develop several significant customizations to the claims base system to meet unique processing requirements. Due in part to additional customizations, the “go live” schedule was extended to late 2002, with some aspects of the system still being fine-tuned. Another consideration of the extended implementation schedule was extension of the HIPAA compliance deadlines.

The claims system is operating in production at MIHS on IBM AS/400 equipment installed specifically for this project. This is MIHS’ first experience with this operating platform and many procedures and technical skills have been updated to support this environment. OAOHS is still heavily involved in maintaining the software environment of the claims system, providing both fixes and enhancements to the application.

Scope and Methodology

The scope of this audit was to determine if controls provide reasonable assurance that:

- Logical access to production data files and programs are restricted to authorized individuals
- Claims application security capabilities and configurations support HIPAA security compliance efforts
- Changes to existing applications and new applications being developed are authorized, tested, approved, properly implemented, and documented
- Integrity of critical system software is maintained

- The computer system is backed up to electronic media and stored off-site on a regular basis, and that procedures are employed to maintain the integrity of electronic storage media.

This audit was performed in accordance with generally accepted government auditing standards.

Department Reported Accomplishments

The following information was provided by Maricopa Integrated Health System (MIHS) for inclusion in this report.

System

MIHS/HP successfully migrated to a fully interfaced system, OAO HealthCare Solutions, which provides real time access to our business information. This system allows detailed audit tracking, instant online document retrieval with the option of unlimited long-term storage; this allows us to streamline needed business processes.

Applications/Products

Current applications allow MIHS/HP to customize product lines to meet customer/business needs and demands. This increased flexibility is a major benefit in our on-going goal of greater cost containment, communication, productivity and member/provider service.

Provider Enhancements

Greatly reduced time and cost associated with information sharing by allowing electronic correspondence with providers via secure email, faxing and automatic letter creation. This system enhancement greatly reduces our human error rate and ensures our information accuracy. Our provider enhancements allow greater communication between MIHS/HP and our Provider Network. We now provide electronic billing, via secure Internet, to our Provider Network. We scan all submitted paper claims to transform them into our electronic format, which allows for greater document processing, archival, and retrieval. These enhancements allow information changes and online status on eligibility, authorizations and claims research for our providers.

Membership Enhancements

Allows electronic downloading/uploading of member eligibility, which greatly reduces human errors and ensures data is current and accurate. Application allows case management for high-risk, chronic and catastrophically ill members. In addition, disease management/patient tracking of specific groups in order to ensure patient education and treatments are in compliance. Allow members a secure Internet lookup of our provider network, claim status and health information.

Issue 1 Claims System Security

Summary

The current claims system lacks effective security controls over user access, system settings, and password parameters. Weak controls over these areas could result in improper disclosure of information. MIHS should strengthen system security controls.

Best Practice

Industry leading practices indicate that user access should be limited to business need only, and be reviewed regularly to determine if account access is appropriate; disabled or unused accounts should be removed.

Security Weakness

Current claims system access controls contain the following weaknesses:

- System operators with security officer permissions have the ability to access any device
- The device session setting (QLMTDEVSSN) is configured to allow a user to sign on to multiple terminals simultaneously
- The restore object-setting (QALWOBJRST) is configured to allow users to restore security-sensitive programs
- The IBM system supplied account (i.e., accounts that start with Q) passwords are inappropriately configured
- The AS/400 object auditing has not been enabled
- The default dedicated service tools (DST) password has not been changed
- Non-support employees/normal end users have special authority rights assigned to their user accounts
- User accounts are not reviewed on a regular basis to determine if access rights are appropriate

The current environment may allow unauthorized changes to data or system resources. The new claims system was not initially set up with best practice security in mind. The actions recommended on the following page will help to ensure that access to data and resources are properly restricted.

Recommendation

MIHS should:

- A.** Change the QLMTSECOFR value from 0 to 1 and explicitly assign device access to the users that have security officer rights.
- B.** Change the device session setting (QLMTDEVSSN) to 1, which limits a user account to one device session.
- C.** Configure the restore object setting (QALWOBRST) to *NONE, which prohibits object restoration. Execute the check object integrity command (CHKOBJITG) to determine if changes are appropriate. This command should be re-executed periodically to determine if changes made on the system are appropriate.
- D.** Configure IBM system supplied accounts with a password of *NONE to prevent unauthorized changes.
- E.** Review AS/400 objects and consider enabling audit logging (QAUDLVL) for the appropriate objects. Some considerations in deciding which objects should be audited include business risk of the object, availability to end users, and systems control risk of the object.
- F.** Retain and review audit logs according to business need and system resources (i.e. logs reviewed weekly; retain logs for at least one month).
- G.** Change the default dedicated service tools (DST) password and limit knowledge of the password to AS/400 support personnel.
- H.** Perform a detailed review of account access rights for all users to determine if access rights have been appropriately configured within MIHS standards and on a business-need only basis. Reviews should be performed on a quarterly basis to maintain appropriate user system access.

Issue 2 Program Change Controls

Summary

The current claims system lacks effective controls over changes to programs. The absence of change and approval documentation, and effective segregation of duties, increases the risk that a program could cause system failure, malfunction, or inaccurate data. MIHS should improve change control procedures.

Best Practices

Industry leading practices include formal change control policies and procedures that outline, in detail, appropriate steps and approvals for application changes and system maintenance. In addition, proper segregation of duties should exist between developers, testers, and implementers.

Current Conditions

Formal Hospital Information Technology (HIT) change control policies and procedures are not documented to outline proper control. Change control documentation and approval is not properly retained. In addition, proper segregation of duties does not exist between developers and the production system. However, management has explained that informal change controls procedures exist that include email approval of program changes for the claims system prior to implementation to production. In addition, HIT is performing information quality assurance testing. End users are generally included in the test work.

Risk

These weaknesses increase the risk that an unauthorized and improperly tested program could be implemented and cause system failure, malfunction, or inaccurate data due to poor coding. The HIT department lacks the knowledge to properly implement code into the production environment. Therefore, HIT is allowing claims application programmers to implement changes into the production environment.

Recommendation

MIHS should develop formalized change management procedures specific to the AS/400 environment and the claims system that includes the following:

- A. Formalized, detailed change control policies and procedures.
- B. Documented milestone sign-off by the appropriate managers and team members.
- C. Documented detail test scripts for use in the quality assurance testing phase.
- D. Random sample auditing to determine if objects/code/changes to production have appropriate documentation and approval.
- E. Segregation of duties between phases of the change control process.

Issue 3 System Software

Summary

The most current software updates have not been installed for the claims system. In addition, software maintenance procedures are not performed on a regular basis. These weaknesses could result in undetected errors or a disruption of business services. MIHS should strengthen controls over system software maintenance activities.

Best Practices

Industry leading practices recommend maintaining computer systems with the most current operating system and patches. They also indicate that formalized maintenance procedures should be documented, followed, and the results recorded on a regular basis.

Patches

The most current OS/400 patches and operating system have not been installed to the claims system. However, HIT management indicated that the patches have not been installed due to limited disk space. Failure to install current updates increases the risk that system resources may fail and cause a disruption of business processes. We understand that the most recent hardware upgrades are scheduled to be implemented soon. This will increase processor performance and disk space capacity and should allow the installation of the most current operating system and patches.

Maintenance Procedures

Formalized AS/400 maintenance procedures are not documented and performed on a regular basis. However, we noted that system operators periodically review and track some AS/400 system parameters and log the results in the Data Center Daily Checklist.

In addition, we noted that IT support resources appear to be insufficient to properly support current AS/400 (claims application) system day-to-day maintenance, support, and system review. This practice presents an elevated risk that a batch or system error may go undetected and cause problems that may have been preventable. This may cause system resources to be unavailable and business processes to be stopped.

Recommendation

MIHS management should:

- A.** Continue with the AS/400 hardware upgrade, operating system upgrade, and patch installation to implement the IBM recommended system environment.
- B.** Create and follow formalized AS/400 maintenance procedures to support batch processes, system performance, and other activities performed in accordance with MIHS business objectives.
- C.** Perform an evaluation of IT resources to determine if additional support personnel are required to perform day-to-day system operations.

Issue 4 Regulatory Compliance

Summary

New healthcare regulations require increased security controls over systems that contain patient information. Some required controls have not yet been implemented. Incomplete security controls increase the risk that MIHS will not be able to meet regulatory requirements. MIHS should identify the additional work to be done and schedule it for completion prior to statutory deadlines.

HIPAA Compliance

Health Insurance Portability and Accountability Act (HIPAA) regulations identify security safeguards that should exist in health care organizations. Although HIT has addressed many of the HIPAA security requirements related to claims system policies and procedures for account creation and user access levels, additional work is required. Incomplete security controls increase the risk that MIHS will not be HIPAA-compliant and might face regulatory sanctions.

HIPAA security requirements were finalized in early 2003, with compliance required by April 10, 2005. Components of the requirements include administrative safeguards such as security awareness and training, security incident procedures, contingency plan, and risk evaluation. Technical safeguards include audit controls and transmission security.

Recommendation

MIHS should implement the following requirements:

- A. Develop policies and procedures in accordance with HIPAA regulations by April 10, 2005.
- B. Include in the safeguards listed above, the designation of a security official and the requirement of conducting a risk analysis to identify key areas of risk.
- C. Implement extensive security controls and policies, disaster recovery plans, and active security technologies.

Issue 5 System Recovery

Summary

System recovery procedures have not been documented and included in the Systems Recovery Procedures or Disaster Recovery Plan. In the event of a disruption of service, MIHS may not be able to recover the system and application in an efficient and timely manner. MIHS should include detailed restoration instructions for the operating system and the claims application in the System Recovery Procedures and the Disaster Recovery Plan.

County Policy Requirements

County Policy A1602 requires that each elected official and appointed department director establish their disaster recovery plans and practices sufficient to ensure that: 1) their information resources are protected, backed-up, and recoverable; and 2) the integrity, availability, and reliability of all electronic assets are not compromised or affected. Departments should develop formal recovery plans and be prepared to implement them.

Operating system and claims system restoration instructions should include detailed command line instructions for restoring the operating system and claims application, vendor contact information for IBM, OAO, and DataPros, and an MIHS notification tree for contacting employees during a disaster.

Risk

The AS/400 (claims system) recovery procedures have not been formally documented and included in the Systems Recovery Procedures or disaster recovery plan. In addition, the following items are not included in the disaster recovery plan:

- Third party contact information (i.e. warm site, vendor contact information, etc.)
- AS/400 recovery information
- Detailed procedures for restoring the claims system

We noted that HIT performs nightly backups of system data and has performed periodic file restoration procedures. However, the disaster recovery procedure is not regularly tested and reviewed.

Recommendation

MIHS management should:

- A. Include detailed AS/400 operating system and claims system restoration instructions in the Systems Recovery Procedure document.
- B. Perform regular disaster recovery tests to determine if documentation and procedures are adequate to restore business operations and meet MIHS disaster recovery objectives.
- C. Document the results and review the results to improve the procedures.**

Department Response

Audit Response
Maricopa Integrated Health System
Claims System

Issue #1

Claims system Security:

The current claims system lacks effective security controls over user access, system settings, and password parameters. Weak controls over these areas could result in improper disclosure of information. MIHS should strengthen system security controls.

Recommendation A:

Change the QLMTSECOFR value from 0 to 1 and explicitly assign device access to the users that have security officer rights.

Response:

Concur -- Completed

Corrected immediately after the audit, once the hardware and software update was completed. The value on QLMTSECOFR was set to 1.

Target Completion Date: 5/10/03 - completed.

Recommendation B:

Change the device session setting (QLMTDEVSSN) to 1, which limits a user account to one device session.

Response:

Concur -- Completed

Corrected immediately after the audit, once the hardware and software update was completed. The value on QLMTDEVSSN was set to 1.

Target Completion Date: 5/10/03 - completed.

Recommendation C:

Configure the restore object setting (QALWOBRST) to *NONE, which prohibits object restoration. Execute the check object integrity command (CHKOBJITG) to determine if changes are appropriate. This command should be re-executed periodically to determine if changes made on the system are appropriate.

Response:

Concur -- Completed

Corrected immediately after the audit. The value on QALWOBRST was set to *NONE.

Target Completion Date: 5/10/03 - completed.

Recommendation D:

Configure IBM system supplied accounts with a password of *NONE to prevent unauthorized changes.

Response:

Concur -- Completed

Corrected immediately after the audit, once the operating system upgrade was completed. The passwords were set to *NONE on all IBM system supplied user accounts.

Target Completion Date: 5/10/03 - completed.

Recommendation E:

Review AS/400 objects and consider enabling audit logging (QAUDLVL) for the appropriate objects. Some considerations in deciding which objects should be audited include business risk of the object, availability to end users, and systems control risk of the object.

Response:

Concur -- in process

A meeting has been scheduled with the OAO team to determine which object will require auditing.

Target Completion Date: 12/31/03

Recommendation F:

Retain and review audit logs according to business need and system resources (i.e. logs reviewed weekly; retain logs for at least one month).

Response:

Concur -- in process

Now that we have adequate disk space capacity, we will retain the logs for one month, and operators will review the logs on weekly basis.

Target Completion Date: 12/31/03

Recommendation G:

Change the default dedicated service tools (DST) password and limit knowledge of the password to AS/400 support personnel.

Response:

Concur -- Completed

Corrected immediately after the audit, once the operating system upgrade was completed. The password on the Dedicated Service Tools (DST) was changed, and password knowledge was limited only to the AS/400 support personnel.

Target Completion Date: 5/10/03 - completed.

Recommendation H:

Perform a detailed review of account access rights for all users to determine if access rights have been appropriately configured within MIHS standards and on a business-need only basis. Reviews should be performed on a quarterly basis to maintain appropriate user system access.

Response:

Concur -- in process

Operations is currently in the process of developing a procedure to audit user accounts on a quarterly basis.

Target Completion Date: 9/01/03

Issue #2:

Program Change Controls:

The current claims system lacks effective controls over changes to programs. The absence of change and approval documentation, and effective segregation of duties, increases the risk that a program could cause system failure, malfunction, or inaccurate data. MIHS should improve change control procedures.

Recommendation A - E:

MIHS should develop formalized change management procedures specific to the AS/400 environment and the claims system that includes the following:

- A. Formalized, detailed change control policies and procedures.
- B. Documented milestone sign-off by the appropriate managers and team members.
- C. Documented detail test scripts for use in the quality assurance-testing phase.
- D. Random sample auditing to determine if objects/code/changes to production have appropriate documentation and approval.
- E. Segregation of duties between phases of the change control process.

Response: Concur – In process

MIHS has a current Change Control Policy/ Procedure that is utilized for all other applications/systems. We are in the process of modifying this procedure to meet the specific needs of the OAO AS/400 system.

The following processes will be include in the procedure:

- Formalized, detailed change control process.
- Sign-off by the appropriate team members, and Managers.
- Back-out procedure.
- Testing/acceptance/implementation process will be included in the procedure
- Auditing policy will be included to determine in Object/code/changes have been properly documented.

Target Completion Date: 12/31/03

Issue #3:

System Software:

The most current software updates have not been installed for the claims system. In addition, software maintenance procedures are not performed on a regular basis. These weaknesses could result in undetected errors or a disruption of business services. MIHS should strengthen controls over system software maintenance activities.

Recommendation A:

Continue with the AS/400 hardware upgrade, operating system upgrade, and patch installation to implement the IBM recommended system environment.

Response:

Concur -- completed
Corrected immediately after the audit.

Target Completion Date: 5/10/03 - completed.

Recommendation B:

Create and follow formalized AS/400 maintenance procedures to support batch processes, system performance, and other activities performed in accordance with MIHS business objectives.

Response:

Concur -- in process
We are in the process of developing a formalized Policy/procedure, which will outline the support requirements for batch processing, system performance tuning, and software implementations.

Target Completion Date: 12/31/03

Recommendation C:

Perform an evaluation of IT resources to determine if additional support personnel are required to perform day-to-day system operations.

Response:

Concur -- in process

Target Completion Date: 9/01/03

Issue #4:

Regulatory Compliance:

New healthcare regulations require increased security controls over systems that contain patient information. Some required controls have not yet been implemented. Incomplete security controls increase the risk that MIHS will not be able to meet regulatory requirements. MIHS should identify the additional work to be done and schedule it for completion prior to statutory deadlines.

Recommendation A:

Develop policies and procedures in accordance with HIPAA regulations by April 10, 2005.

Response:

Concur -- in process

Target Completion Date: 4/10/05

Recommendation B:

Include in the safeguards listed above, the designation of a security official and the requirement of conducting a risk analysis to identify key areas of risk.

Response:

Concur -- in process

Target Completion Date: 4/10/05

Recommendation C:

Implement extensive security controls and policies, disaster recovery plans, and active security technologies.

Response:

Concur -- in process

Target Completion Date: 4/10/05

Issue #5:

System Recovery:

System recovery procedures have not been documented and included in the Systems Recovery Procedures or Disaster Recovery Plan. In the event of a disruption of service, MIHS may not be able to recover the system and application in an efficient and timely manner. MIHS should include detailed restoration instructions for the operating system and the claims application in the System Recovery Procedures and the Disaster Recovery Plan.

Recommendation A:

Include detailed AS/400 operating system and claims system restoration instructions in the Systems Recovery Procedure document.

Claims System Audit Response – July 8, 2003

and the claims application in the System Recovery Procedures and the Disaster Recovery Plan.

Recommendation A:

Include detailed AS/400 operating system and claims system restoration instructions in the Systems Recovery Procedure document.

Response:

Concur -- completed

Corrected immediately after the audit. The requirements for the AS/400 System Recovery were included in our current system shutdown, startup, and disaster recovery procedures.

Target Completion Date: 5/10/03 - completed.

Recommendation B:

Perform regular disaster recovery tests to determine if documentation and procedures are adequate to restore business operations and meet MIHS disaster recovery objectives.

Response:

Concur -- in process

Target Completion Date: 5/10/04

Recommendation C:

Document the results and review the results to improve the procedures.

Response:


Concur -- in process

Target Completion Date: 5/10/04

Approved By :


Department Head/Elected Official

7-10-03
Date


Chief Officer

7/15/03
Date


County Administrative Officer

7/20/03
Date